Trials@uspto.gov
571.272.7822

Paper 29
Entered: February 1, 2022

UNITED STATES PATENT AND TRADEMARK OFFICE

---

BEFORE THE PATENT TRIAL AND APPEAL BOARD

---

DOLBY LABORATORIES, INC.,
Petitioner,

v.

INTERTRUST TECHNOLOGIES CORPORATION,
Patent Owner.

---

IPR2020-00665
Patent 8,931,106 B2

---

Before MICHAEL R. ZECHER, NABEEL U. KHAN, and CHRISTOPHER L. OGDEN, *Administrative Patent Judges*.

ZECHER, *Administrative Patent Judge*.

# JUDGMENT
Final Written Decision
Determining Only Challenged Claim Unpatentable
*35 U.S.C. § 318(a)*

# I. INTRODUCTION

Petitioner, Dolby Laboratories, Inc. ("Dolby"), filed a Petition requesting an *inter partes* review ("IPR") of independent claim 17 of U.S. Patent No. 8,931,106 B2 (Ex. 1001, "the '106 patent"). Paper 2 ("Pet."). Patent Owner, Intertrust Technologies Corporation ("Intertrust"), filed a Preliminary Response. Paper 6 ("Prelim. Resp."). With our authorization, Dolby filed a Preliminary Reply (Paper 7), and Intertrust filed a Preliminary Sur-reply (Paper 8), each of which were tailored narrowly to address the non-exclusive list of six factors set forth in *Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 11 (PTAB Mar. 20, 2020) (precedential) (Order authorizing supplemental briefing) that we consider in determining whether to exercise our discretion to institute an IPR when there is a related district court case involving the same patent. Taking into account the arguments presented in Intertrust's Preliminary Response together with the arguments presented in the authorized briefing, we determined that the information presented in the Petition established that there was a reasonable likelihood that Dolby would prevail with respect to independent claim 17 of the '106 patent. Pursuant to 35 U.S.C. § 314, we instituted this *inter partes* review on February 16, 2021, as to this challenged claim and all grounds raised in the Petition. Paper 11 ("Institution Decision" or "Dec. on Inst.").

During trial, Intertrust filed a Patent Owner Response (Paper 19, "PO Resp."), Dolby filed a Reply to the Patent Owner Response (Paper 21, "Pet. Reply"), and Intertrust filed a Sur-reply to the Reply (Paper 24, "PO Sur-reply"). An oral hearing was held on November 16, 2021, and a transcript of the hearing is included in the record. Paper 28 ("Tr.").

We have jurisdiction under 35 U.S.C. § 6. This decision is a Final Written Decision under 35 U.S.C. § 318(a) as to the patentability of independent claim 17 of the '106 patent. For the reasons we identify below, we hold that Dolby has demonstrated by a preponderance of the evidence that this challenged claim is unpatentable.

*A. Related Matters*

The parties indicate that the '106 patent is the subject of the following four district court cases: (1) *Dolby Laboratories, Inc. v. Intertrust Corp.*, No. 3:19-cv-03371 (N.D. Cal.); (2) *Intertrust Technologies Corp. v. AMC Entertainment Holdings, Inc.*, No. 2:19-cv-00265 (E.D. Tex.); (3) *Intertrust Technologies Corp. v. Cinemark Holdings, Inc.*, No. 2:19-cv-00266 (E.D. Tex.); and (4) *Intertrust Technologies Corp. v. Regal Entertainment Group*, No. 2:19-cv-00267 (E.D. Tex.). Pet. 6; Paper 3, 2.[1] In the claim construction section below, we refer to the declaratory judgment of non-infringement filed by Dolby in the U.S. District Court for the Northern District of California as the "California Action."

*B. The '106 Patent*

The '106 patent, titled "Systems and Methods for Managing and Protecting Electronic Content and Applications," issued from U.S. Patent Application No. 12/728,098 ("the '098 application"), filed on March 19, 2010. Ex. 1001, codes (54), (21), (22). The '098 application includes an extensive chain of priority that ultimately results in it claiming the benefit of

[1] Intertrust's Mandatory Notices filed in accordance with 37 C.F.R. § 42.8 does not include page numbers. Paper 3. We consider the Title page as page 1 and then proceed from there in numerical order.

U.S. Provisional Patent Application No. 60/210,479, filed on June 9, 2000. *Id.* at code (63), 1:7–12.

The '106 patent generally relates to "managing electronic content" and, in particular, to "systems and methods . . . for governing electronic content and applications through the use of electronic credentials and certification procedures." Ex. 1001, 1:26–30. According to the '106 patent, "[w]ith the advent of the Internet and the prevalent use of electronic systems, increased attention has been paid to protecting the interests of content owners and . . . ensuring that the integrity of electronic transactions is not compromised." *Id.* at 1:34–37. The '106 patent addresses these and other problems by "providing content creators, application developers, consumers, and regulators with increased power and flexibility to define and create efficient markets for the exchange, control, and protection of digital goods and for the performance of electronic transactions." *Id.* at 1:48–53.

Figure 1 of the '106 patent, reproduced below, "illustrates a system for certifying and credentialing applications in accordance with [one] embodiment." Ex. 1001, 2:49–51, 3:45–46.

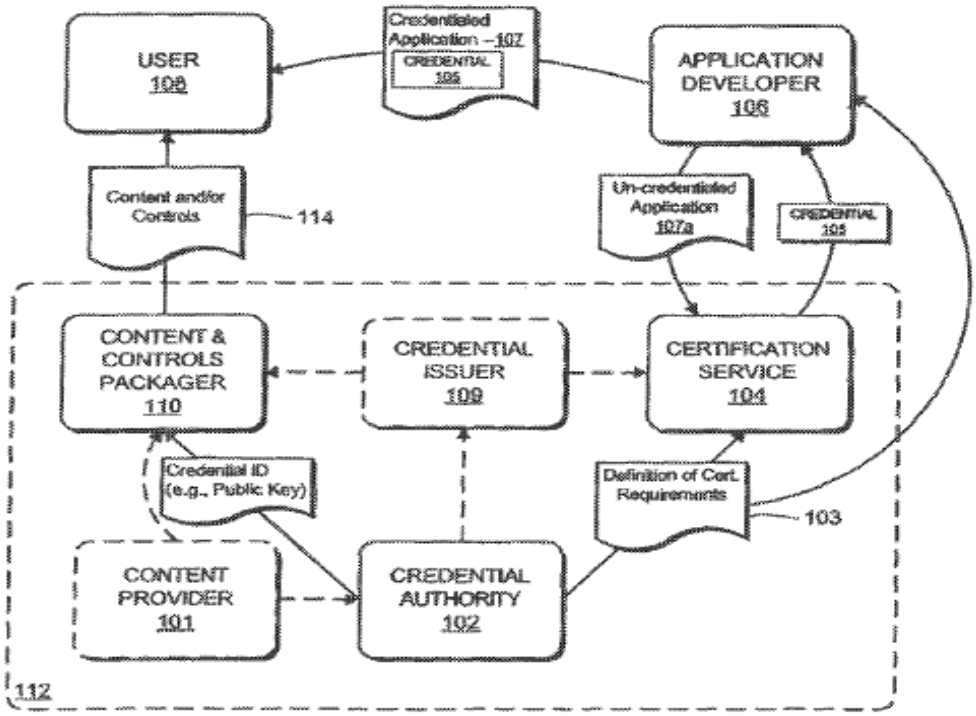



FIG. 1

Figure 1, reproduced above, illustrates a rights management system that includes credential authority 102 that defines certain requirements 103 that applications must meet to receive a credential. *Id.* at 3:46–48. "Application developer 106 creates . . . application 107*a* that conforms to requirements 103 and provides" this application to certification service 104. *Id.* at 3:61–63. Certification service 104 "analyzes and tests application 107*a* to make sure that it meets . . . requirements 103 specified by credential authority 102." *Id.* at 3:63–65. If application 107*a* meets these requirements, it is given credential 105, thereby allowing "application developer 106 [to] distribute . . . credentialed application 107 to . . . application user 108." *Id.* at 3:65–4:2; *see also id.* at Fig. 8 (illustrating credentials 802, 812 with

multiple attributes). "Credential authority 102 also issues a copy of its credential ID [identification] and/or related identification data . . . to content and controls package 110," which, in turn, uses this information "to create controls that can be associated with the content provider's content." *Id.* at 4:3–10. Notably, the '106 patent discloses that content provider 101 may "choose to condition an application program's access to content on the . . . possession of a suitable combination of credentials, the credentials originating from a variety of credential authorities and/or certification services and attesting to the application's compliance with the authorities' specifications and requirements." *Id.* at 7:11–17.

The '106 patent further discloses that, "[w]hen user 108 attempts to use application 107 to process content 114, the user's system checks application 107 for the presence of the appropriate credential 105." Ex. 1001, 4:21–23. "If the [appropriate] credential 105 is present, . . . application 107 may proceed with using content 114," whereas "[i]f credential 105 is not present, use of content 114 can be prohibited." *Id.* at 4:23–26. Stated differently, when credential 105 from credential authority 102 is associated securely with application 107, "and content 114 is associated with a rule requiring credential 105 to be present as a condition of granting application 107 access to the content," "users 108 and content providers 101 can be confident, within the security bounds of the certification process and/or the credential," that application 107 will operate in accordance with the requirements and specifications established by credential authority 102. *Id.* at 4:26–34.

Figure 6 of the '106 patent, reproduced below, illustrates a system that uses credentials to manage electronic content and applications in accordance with another embodiment. Ex. 1001, 2:62–64, 10:17–18.

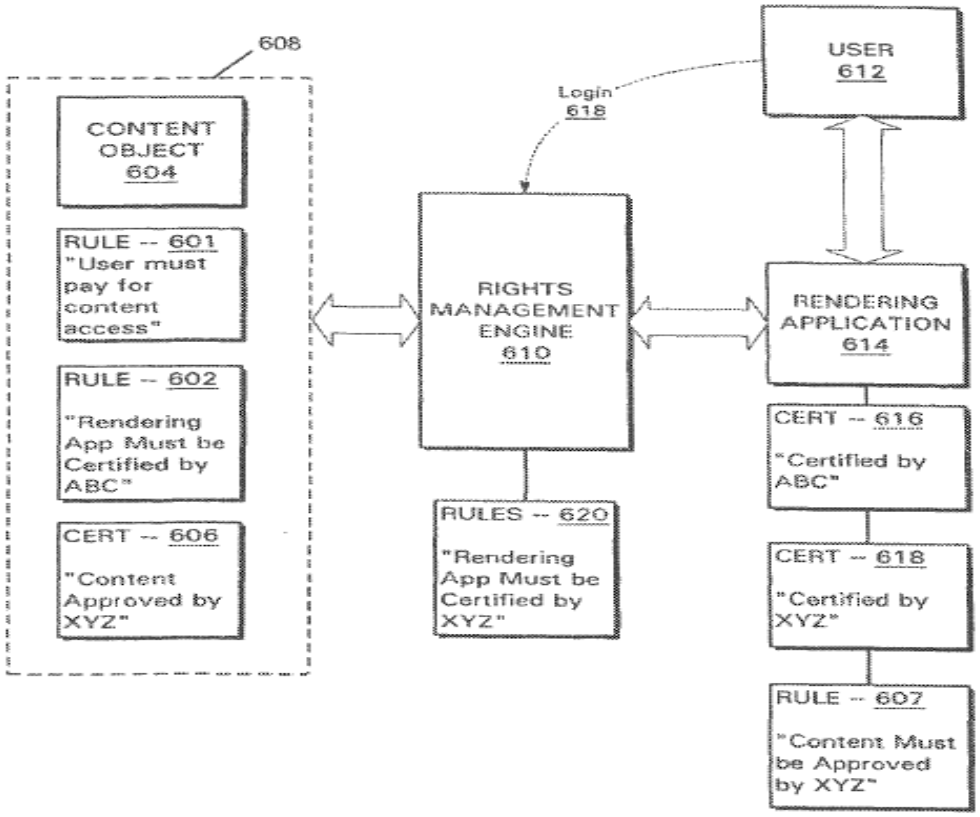



FIG. 6

Figure 6, reproduced above, illustrates a system that includes user 612 employing "rendering application 614 to access content [object] 604" that "is securely packaged and associated with rules 601, 602 that govern how the content can be used." *Id.* at 10:18–21. "[W]hen . . . user 612 requests access to content [object] 604 via . . . rendering application 614, the request is routed to . . . rights management engine 610." *Id.* at 10:49–51. "Rights management engine 610 detects the association between rules 601, 602 and

content object 604, and evaluates whether the conditions specified by the rules have been satisfied." *Id.* at 10:51–54. Alternatively, rule 620 may be separately delivered to rights management engine 610, "rule [620] indicating that in order for . . . rendering application 614 to receive decrypted content, it must be certified by XYZ, certification by XYZ signifying that the application was designed to check for . . . certificate 606 before releasing content 604." *Id.* at 11:16–23. After determining that the rules governing access to content object 604 have been satisfied, "rights management engine 610 may release content [object] 604 to rendering application 614" by decrypting the content. *Id.* at 10:58–61; *see also id.* at 11:2–3 ("[I]t may be desirable to certify that [rendering] application 614 will check content [object] 604 for the appropriate certificate 606 before presenting the content to . . . user 612.").

### *C. Challenged Claim*

Independent claim 17 is the only challenged claim and is reproduced below:

> 17. A method for managing the use of electronic content at a computing device, the method including:
>
> receiving a piece of electronic content;
>
> receiving, separately from the piece of electronic content, data specifying one or more conditions associated with rendering the piece of electronic content, the one or more conditions including a condition that the piece of electronic content be rendered by a rendering application associated with a first digital certificate;
>
> executing a rendering application on the computing device, the rendering application being associated with at least the first digital certificate, the first digital certificate having been generated by a first entity based at least in part on a determination

that the rendering application will handle electronic content with at least a predefined level of security;

requesting, through a rights management engine executing on the computing device, permission for the rendering application to render the piece of electronic content;

determining, using the rights management engine, whether the one or more conditions specified by the data have been satisfied;

decrypting the piece of electronic content; and

rendering the decrypted piece of electronic content using the rendering application.

Ex. 1001, 19:25–20:16.

*D. Asserted Prior Art References*

Dolby relies on the prior art references set forth in the tables below.

Pet. 9–10.

| Name[2] | Reference | Dates | Exhibit No. |
|---|---|---|---|
| Hurtado | US 6,611,812 B2 | issued Aug. 26, 2003; filed Aug. 17, 1999 | 1005 |
| Shear | WO 98/10381 | published Mar. 12, 1998; filed Sept. 4, 1996 | 1006 |

[2] For clarity and ease of reference, we only list the first named inventor.

| Name[2] | Reference | Dates | Exhibit No. |
|---|---|---|---|
| Peinado | US 6,772,340 B1 | issued Aug. 3, 2004; filed Mar. 15, 2000[3] | 1007 |

*E. Asserted Grounds of Unpatentability*

Dolby challenges claim 17 of the '106 patent based on the asserted grounds of unpatentability set forth in the table below. Pet. 10, 30–89.

| Claim Challenged | 35 U.S.C. § | Reference(s) |
|---|---|---|
| 17 | 103(a)[4] | Peinado |
| 17 | 103(a) | Peinado, Shear |
| 17 | 103(a) | Hurtado, Peinado |
| 17 | 103(a) | Hurtado, Peinado, Shear |

[3] Peinado issued from U.S. Patent Application No. 09/526,290, which claims priority to U.S. Provisional Application No. 60/176,425 ("the '425 application"), filed on January 14, 2000. Ex. 1007, codes (21), (60). Dolby contends that Peinado qualifies as prior to the '106 patent under 35 U.S.C. § 102(e) because the '425 application "describes all of Peinado's subject matter and supports at least Peinado's claim 1." Pet. 9 (citing Ex. 1013 (comparing the disclosures of Peinado and the '425 application); Ex. 1014 (table illustrating how the '425 application provides sufficient written description support for independent claim 1 of Peinado)). During trial, Intertrust does not contest that the '106 patent is entitled to claim priority back to the '425 application, filed on January 14, 2000. *See* PO Resp.; PO Sur-reply.

[4] The Leahy-Smith America Invents Act ("AIA"), Pub. L. No. 112-29, 125 Stat. 284, 287–88 (2011), amended 35 U.S.C. § 103, effective March 16, 2013. Because the '106 patent issued from the '098 application, which was filed before this date, the pre-AIA version of § 103 applies. Ex. 1001, codes (21), (22).

## II. ANALYSIS

### *A. Claim Construction*

In an *inter partes* review proceeding based on a petition filed on or after November 13, 2018, such as here, claim terms are construed using the same claim construction standard as in a civil action under 35 U.S.C. § 282(b). *See* 37 C.F.R. § 42.100(b) (2019). That is, claim terms generally are construed in accordance with their ordinary and customary meaning, as understood by a person of ordinary skill in the art, and the prosecution history pertaining to the patent at issue. *Id.* The ordinary and customary meaning of a claim term "is its meaning to the ordinary artisan after reading the entire patent," and "as of the effective filing date of the patent application." *Phillips v. AWH Corp.*, 415 F.3d 1303, 1313, 1321 (Fed. Circ. 2005) (en banc).

In its Petition, Dolby proposes that we construe the claim term "digital certificate" as "an electronic credential of an authority." Pet. 28. To support its proposed construction, Dolby argues that the specification of the '106 patent uses the words "certificate" and "credential" interchangeably. *Id.* (citing Ex. 1001, 5:16–18). Dolby also directs us to certain disclosures in the specification of the '106 patent and the supporting testimony of its declarant, Sandeep Chatterjee, Ph.D., indicating that applications, content, and/or users may be given credentials by satisfying certain requirements or by demonstrating that they have certain predefined characteristics. *Id.* at 28–29 (citing Ex. 1001, code (57), 3:38–39, 3:48–55, 4:40–43, 4:51–53, 7:1–3,

10:26–33, 10:38–41, 12:60–61; Ex. 1002 (Declaration of Dr. Chatterjee in support of Petition) ¶¶ 62–69).

In its Patent Owner Response, Intertrust contends that Dolby's proposed construction of the claim term "digital certificate" "is overbroad and misleading." PO Resp. 20. According to Intertrust, Dolby proposed the same construction in the California Action, but Intertrust countered by proposing that this term should be given its plain and ordinary meaning of "digitally signed data that attests to a relationship between two or more pieces of information." *Id.* at 19. Intertrust, however, argues that the district court in the California Action did not construe the claim term "digital certificate" because it was not one of the ten terms the parties identified as being the "most significant to the resolution of that case." *Id.*

Despite the district court in the California Action not construing the claim term "digital certificate," Intertrust represents that it identified two technical dictionary definitions that it submitted in the California Action that purportedly support construing this term for purposes of this proceeding in accordance with its plain and ordinary meaning. PO Resp. 20 (citing Ex. 2033 (Declaration of Dr. Markus Jakobsson in support of Patent Owner Response) ¶¶ 75–77). Intertrust also notes that Hurtado, which is one of the prior art references asserted by Dolby in this proceeding, provides a definition of a "digital certificate" that is consistent with (1) both of the two dictionary definitions of a "digital certificate" that Intertrust submitted in the California Action, and (2) with how the '106 patent uses this term throughout the specification. *Id.* (citing Ex. 1005, 17:23–31; Ex. 2033 ¶ 78). According to Intertrust, the two dictionary definitions of a "digital certificate" submitted in the California Action and Hurtado's definition of

this same term collectively illustrate that, even though "a digital certificate is a type of credential, not all credentials are digital certificates." *Id.* Nevertheless, Intertrust asserts that it "believes construction of the term is not necessary to resolve the parties' controversy, and the term should be afforded its plain and ordinary meaning." *Id.* at 20–21.

In its Reply, Dolby disagrees that its proposed construction of the claim term "digital certificate" improperly conflates "certificate" with "credential." Pet. Reply 1. Dolby reiterates that Intertrust fails to take into consideration that the specification of the '106 patent uses these two words interchangeably. *Id.* at 1–2 (citing Ex. 1001, 5:15–20). Accordingly, Dolby asserts that we should adopt its proposed construction set forth in the Petition. *Id.* (citing Pet. 28–29; Ex. 1002 ¶¶ 62–69).

During oral argument, we attempted to clarify each party's position regarding the construction of the claim term "digital certificate." First, during its main presentation, we asked Dolby if we need to construe the claim term "digital certificate" "for purposes of applying the teachings of Peinado and Hurtado." Tr. 7:1–19. In response, counsel for Dolby stated that "[c]ertainly not for the Peinado grounds" because "Peinado discloses a certificate." *Id.* at 7:10–8:7. Later, during its main presentation, we asked Intertrust if it "dispute[s] that the certificate 72 that's in Peinado is a digital certificate, or would . . . qualify as one." *Id.* at 31:26–32:5. In response, counsel for Intertrust stated that, "with respect to Peinado, there is not a dispute that . . . certificate 72 is a digital certificate." *Id.* at 33:7–10.

After considering the fully developed trial record, the issues raised by the parties do not turn on the construction of the claim term "digital certificate." Instead, the issues turn on whether Peinado teaches "the first

digital certificate having been generated by a first entity based at least in part on a determination that the rendering application will handle electronic content with at least a predefined level of security," as recited in independent claim 17. That is, we need not construe the claim term "digital certificate" to determine whether Dolby has demonstrated by a preponderance of the evidence that independent claim 17 of the '106 patent is unpatentable under § 103(a) as obvious over the teachings of Peinado alone or in combination with the teachings of Shear because the parties do not dispute that Peinado's certificate 72 is a digital certificate. *See, e.g.*, *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) ("[W]e need only construe terms 'that are in controversy, and only to the extent necessary to resolve the controversy.'" (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999))).

*B. Obviousness Over the Combined Teachings of Peinado*

Dolby contends that independent claim 17 of the '106 patent is unpatentable under § 103(a) as obvious over the teachings of Peinado. Pet. 30–56. Dolby contends that the teachings of Peinado account for the subject matter of this challenged claim, and provides reasoning as to why a person of ordinary skill in the art would have been prompted to modify this reference. Pet. 30–56; Pet. Reply 2–13. Dolby also relies on the Declaration of Dr. Chatterjee accompanying the Petition to support its positions. Ex. 1002.

During trial, Intertrust contends that the teachings of Peinado do not account for all the limitations recited in independent claim 17. PO Resp. 22–37; PO Sur-reply 3–11. Intertrust relies on the Declaration of Dr.

Jakobsson accompanying the Patent Owner Response to support its positions. Ex. 2033.

We begin our analysis with the principles of law that generally apply to an obviousness ground, an assessment of the level of skill in the art, followed by a brief overview of Peinado, and then we address the parties' contentions with respect to independent claim 17.

*1. Principles of Law*

A claim is unpatentable under § 103(a) if the differences between the claimed subject matter and the prior art are such that the subject matter, as a whole, would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). The question of obviousness is resolved on the basis of underlying factual determinations, including (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of skill in the art; and (4) when in evidence, objective indicia of non-obviousness (i.e., secondary considerations, such as commercial success, long-felt but unsolved needs, failure of others, etc.). *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966). We analyze the asserted grounds based on obviousness with the principles identified above in mind.

*2. Level of Skill in the Art*

In determining the level of skill in the art, various factors may be considered, including the "type of problems encountered in the art; prior art solutions to those problems; rapidity with which innovations are made; sophistication of the technology; and educational level of active workers in the field." *In re GPAC, Inc.*, 57 F.3d 1573, 1579 (Fed. Cir. 1995) (citation

omitted). Relying on the testimony of Dr. Chatterjee, Dolby argues the following:

> a [person of ordinary skill in the art], at the time the '106 patent was filed, would have been a person who . . . had a background in electronic data protection and distribution, a minimum of a bachelor of science's degree in computer science, electrical engineering, mathematics, or a related field, and approximately two years of professional experience or equivalent study in the design of secured electronic systems. Additional graduate education could substitute for professional experience, or significant experience in the field could substitute for formal education.

Pet. 27–28 (citing Ex. 1002 ¶¶ 1–27).

In its Patent Owner Response, Intertrust offers essentially the same assessment of the level of skill in the art as Dolby, arguing the following:

> [a] person of ordinary skill in the art . . . relevant to the '106 patent at the time of the invention would have a Bachelor of Science degree in electrical engineering and/or computer science, and three years of work or research experience in the field of digital rights management ("DRM"), or a Master's degree in electrical engineering and/or computer science and two years of work or research experience in DRM.

PO Resp. 17. Nevertheless, Intertrust asserts that the positions set forth in its Patent Owner Response "would be the same under either party's proposal." *Id.*

We do not discern a material difference between the assessments of the level of skill in the art advanced by either party, nor does either party premise its arguments exclusively on its own assessment. For purposes of this Final Written Decision, we adopt Dolby's assessment, except that we delete the qualifier "a minimum" to eliminate vagueness as to the appropriate level of education. The qualifier expands the range without an

upper bound (i.e., encompassing a Ph.D. degree and beyond), and does not meaningfully indicate the level of skill in the art. Dolby's assessment—without the qualifier—is supported by the testimony of Dr. Chatterjee and it is consistent with the '106 patent and the asserted prior art. We note, however, that our obviousness analysis would be the same under each party's assessment.

*3. Overview of Peinado*

Peinado generally relates to "an architecture for enforcing rights in digital content" and, in particular, to "an enforcement architecture that allows access to encrypted digital content only in accordance with parameters specified by license rights acquired by a user of the digital content." Ex. 1007, 1:37–42. Figure 1 of Peinado, reproduced below, illustrates a block diagram of "an enforcement architecture in accordance with one embodiment." *Id.* at 4:11–13, 5:14–17.

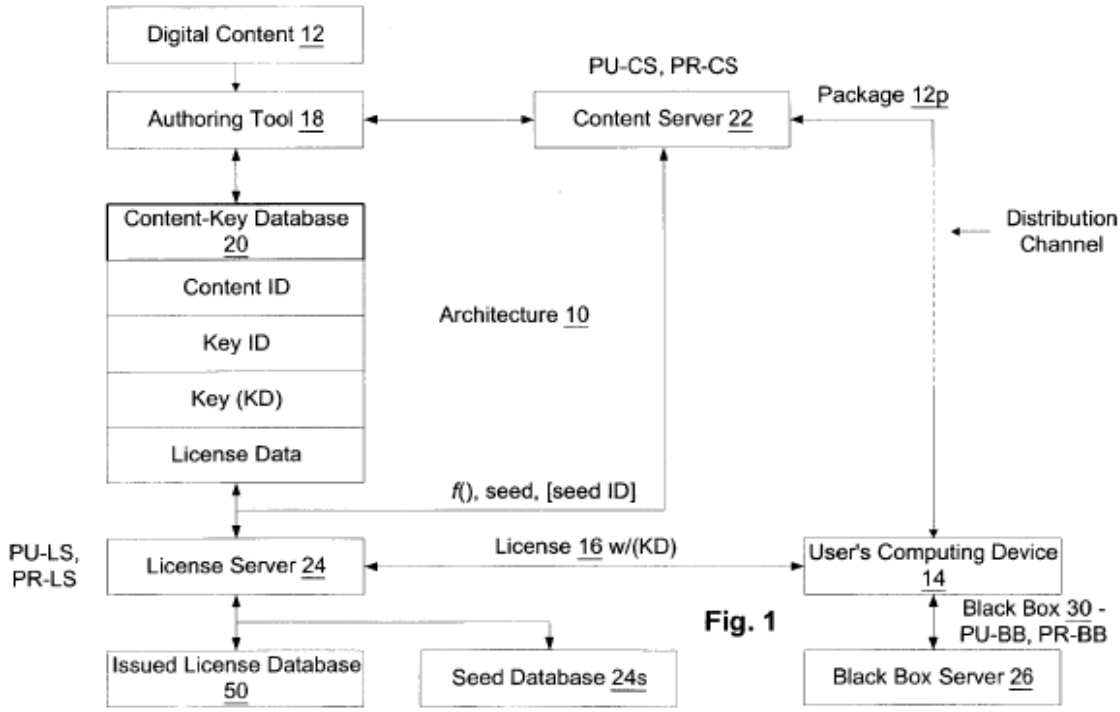



Fig. 1

Figure 1, reproduced above, illustrates how "enforcement architecture 10 allows an owner of digital content 12 to specify license rules that must be satisfied before such digital content 12 is allowed to be rendered on . . . user's computing device 14." *Id.* at 5:18–21. License rules are embodied within digital license 16 that user's computing device 14 obtains from license server 24. *Id.* at 5:21–24.

Peinado discloses that a content owner uses authoring tool 18 to package a piece of digital content 12 by providing the authoring tool with the digital content, instructions and/or rules that accompany the digital content, and instructions and/or rules for packaging the digital content. Ex. 1007, 7:14–21. Authoring tool 18 then produces digital content package 12*p*, which includes both digital content 12 encrypted with a key and the instructions and/or rules that accompany the digital content. *Id.* at 7:21–24. Content server 22 distributes, or otherwise makes available for retrieval, content package 12*p* produced by authoring tool 18 by way of "any appropriate distribution channel," such as "the Internet or another network, an electronic bulletin board, electronic mail, or the like." *Id.* at 9:58–67.

Peinado further discloses that license server 24 receives a request for license 16 from user's computing device 14 in connection with a piece of digital content 12, determines whether the user's computing device can be trusted to honor an issued license, negotiates a license, constructs the license, and then transmits the license to the user's computing device. Ex. 1007, 11:41–49. Preferably, "transmitted license 16 includes the decryption key (KD) for decrypting . . . digital content 12." *Id.* at 11:49–51.

Figure 4 of Peinado, reproduced below, illustrates a block diagram of user's computing device 14 in accordance with one embodiment. Ex. 1007, 4:21–23, 12:65–13:2.

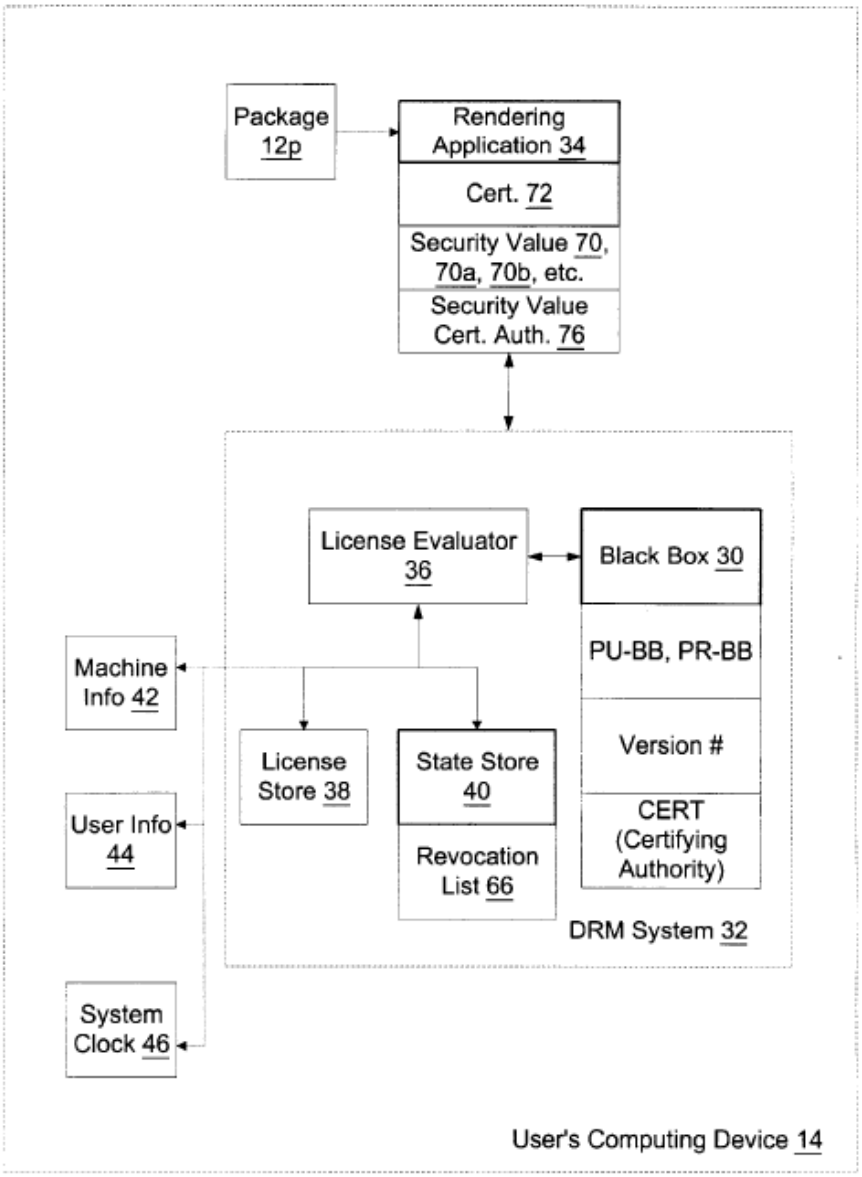



**Fig. 4**

Figure 4, reproduced above, illustrates that user's computing device 14 includes, among other things, Digital Rights Management ("DRM") system 32 and rendering application 34. *Id.* at 13:14–19, 13:59–63, 14:44–57.

When user's computing device 14 requests to render digital content 12, DRM system 32 determines whether the user has license 16 to render the digital content in the manner sought and, if not, obtains a valid license, when necessary, that grants the user the right to play the digital content. *Id.* at 13:20–27. Once it is determined that the user has the right to play digital content 12 in accordance with license 16, DRM system 32 grants computing device 14's request to decrypt the digital content for rendering purposes. *Id.* at 13:27–29. Importantly, Peinado explains that the rights description in each license 16 determines whether user's computing device 14 has rights to play digital content 12 based on any of several factors, including "who the user is, where the user is located, what type of computing device 14 the user is using, what rendering application 34 is calling . . . DRM system 32, the date, the time, etc." *Id.* at 17:61–67; *see also id.* at Fig. 17 (illustrating various steps performed during security approval of rendering application 34), 38:55–40:65 (corresponding description of Figure 17).

*4. Claim 17*

The preamble of independent claim 17 recites "[a] method for managing the use of electronic content at a computing device." Ex. 1001, 19:25–26. To the extent the preamble should be treated as limiting, Dolby contends that Peinado teaches the features recited in the preamble because it discloses user's computing device 14 that allows access to digital content 12 only in accordance with parameters specified by the rights description in license 16. Pet. 41–42 & n.18 (citing Ex. 1007, code (57), 1:37–42, 2:30–53, 13:14–19, 13:29–31, Fig. 4; Ex. 1002 ¶¶ 105–10).

The first step of independent claim 17 recites "receiving a piece of electronic content." Ex. 1001, 19:27. Dolby contends that Peinado teaches

this limitation because it discloses user's computing device 14 obtaining digital content 12 by downloading it from content server 22. Pet. 42–43 (citing Ex. 1001, 13:41–58, Fig. 1; Ex. 1002 ¶¶ 111, 112).

The second step of independent claim 17 recites "receiving, separately from the piece of electronic content, data specifying one or more conditions associated with rendering the piece of electronic content, the one or more conditions including a condition that the piece of electronic content be rendered by a rendering application associated with a first digital certificate." Ex. 1001, 19:28–33. Dolby contends that Peinado teaches "receiving, separately from the piece of electronic content, data specifying one or more conditions associated with rendering the piece of electronic content" because it discloses user's computing device 14 receiving license 16, which includes, among other things, security requirement 68 and trusted security value certifying authority 74, from license server 24 as a separate action from downloading digital content 12 from content server 22. Pet. 43–45 (citing Ex. 1007, 17:60–67, 38:44–40:65, Figs. 1, 8; Ex. 1002 ¶¶ 113–17). Dolby further contends that Peinado teaches "the one or more conditions including a condition that the piece of electronic content be rendered by a rendering application associated with a first digital certificate" because, as one example, Peinado discloses that license 16 includes trusted security value certifying authority 74 that indicates which certifying authorities 76 that issue certificate 72 to rendering application 34 are trustworthy. *Id.* at 45–47 (citing Ex. 1007, 39:33–46, 40:39–48, Fig. 17 (steps 1709–15); Ex. 1002 ¶¶ 118–21).

> The third step of independent claim 17 recites the following:
>
> executing a rendering application on the computing device, the rendering application being associated with at least the first digital certificate, the first digital certificate having been generated by a first entity based at least in part on a determination that the rendering application will handle electronic content with at least a predefined level of security.

Ex. 1001, 20:1–7. Dolby contends that Peinado teaches "executing a rendering application on the computing device" because it discloses "rendering application 34 . . . running on [user's] computing device 14." Pet. 47–48 (quoting Ex. 1007, 13:59–63) (citing Ex. 1007, 14:16–34, 24:36–39, Fig. 4; Ex. 1002 ¶¶ 122–24) (alteration in original).

Dolby further contends that Peinado teaches "the rendering application being associated with at least the first digital certificate, the first digital certificate having been generated by a first entity based at least in part on a determination that the rendering application will handle electronic content with at least a predefined level of security" because it discloses that rendering application 34 is associated with certificate 72, and certifying authority 76 generates this certificate based, at least in part, on a predefined level of security (e.g., a security value of "A" that corresponds to a security value of 90 or higher). Pet. 48–50 (citing Ex. 1007, 38:60–39:3, 39:19–25, 39:56–65; Ex. 1002 ¶¶ 127–29). Dolby also argues that Peinado's letter scales corresponding to a range of security values (e.g., A, B+, AAA, etc.) are consistent with the certification levels provided for the applications disclosed in the '106 patent. *Id.* at 49 n.20 (citing Ex. 1001, 15:52–63).

Alternatively, Dolby contends that, to the extent Peinado does not disclose explicitly a first entity generating a certificate based, at least in part, on a determination that the rendering application handles electronic content

with at least a predefined security level, a person of ordinary skill in the art would have modified Peinado's "certifying authority 76 to conditionally generate a certificate if rendering application 34 is determined to handle content with at least a predefined level of security." Pet. 50 (citing Ex. 1002 ¶ 130). According to Dolby, after determining that Peinado's rendering application 34 has a predefined level of security, certifying authority 76 issues certificate 72 with a corresponding security value and attaches it to the rendering application. *Id.* at 50–51 (citing Ex. 1007, 39:19–25, 39:56–65, Figs. 4, 5B, 8; Ex. 1002 ¶ 131).

Dolby asserts that conditionally issuing certificate 72 establishing a predefined security level to Peinado's rendering application 34, if such a predefined security level is observed, was well-known in the art, as evidenced by the teachings of Ginter, Jobber, and Shear. Pet. 37–38 (citing Ex. 1032; Ex. 1033, 19–20, 28; Ex. 1006, 72:19–22; Ex. 1002 ¶¶ 97, 98). Dolby then proceeds to identify certain benefits that would have resulted from modifying Peinado in this way, which include excluding rendering applications whose security level is below a predefined security level, accounting for the preferences of particular content providers, ensuring more efficient utilization of computational resources, and preventing exposure to security risks. *Id.* at 38–39 (citing Ex. 1002 ¶¶ 99–102). Lastly, Dolby argues that a person of ordinary skill in the art would have had a reasonable expectation of success in modifying Peinado because certifying authority 76 already determines the security values of rendering application 34 and modifying that process to screen or reject rendering applications that do not meet a predefined security level "requires only routine skill." *Id.* at 39–40 (citing Ex. 1002 ¶¶ 103, 104).

The fourth step of independent claim 17 recites "requesting, through a rights management engine executing on the computing device, permission for the rendering application to render the piece of electronic content." Ex. 1001, 20:8–10. Dolby contends that Peinado teaches this limitation because it discloses that user's computing device 14 initiates a request to render digital content 12 either by requesting license 16 or by requesting that license evaluator 36 of DRM system 32 examines license 16 that already exists. Pet. 51–53 (citing Ex. 1007, 13:29–32, 14:31–34, 15:4–19, 18:41–46, 24:10–13, 34:4–8, Fig. 4; Ex. 1002 ¶¶ 135–40).

The fifth step of independent claim 17 recites "determining, using the rights management engine, whether the one or more conditions specified by the data have been satisfied." Ex. 1001, 20:11–13. Dolby contends that Peinado teaches this limitation because it discloses that DRM system 32 verifies that rendering application 34 meets certain security conditions by, as one example, comparing the trusted security value certifying authority 74 in license 16 with the certifying authority 76 that issued certificate 72. Pet. 53–54 (citing Ex. 1007, 40:28–34, 40:49–57, Fig. 17 (steps 1709–15); Ex. 1002 ¶¶ 141, 142).

The sixth step of independent claim 17 recites "decrypting the piece of electronic content." Ex. 1001, 20:14. Dolby contends that Peinado teaches this limitation because it discloses that, after DRM system 32 approves rendering application 34 by verifying that it meets certain security conditions, it decrypts digital content 12. Pet. 54–55 (citing Ex. 1007, 15:10–15, 23:64–24:1, 24:36–39, Fig. 5B; Ex. 1002 ¶¶ 143, 144).

The seventh step of independent claim 17 recites "rendering the decrypted piece of electronic content using the rendering application."

Ex. 1001, 20:15–16. Dolby contends that Peinado teaches this limitation because it discloses that rendering application 34 renders decrypted digital content 12. Pet. 55–56 (citing Ex. 1007, 24:36–39, Fig. 5B (step 535); Ex. 1002 ¶¶ 145, 146).

During trial, Intertrust contends that the teachings of Peinado do not account for the following limitations recited in independent claim 17: (1) "a condition that the piece of electronic content be rendered by a rendering application associated with a first digital certificate"; (2) "the rendering application being associated with at least the first digital certificate, the first digital certificate having been generated by a first entity based at least in part on a determination that the rendering application will handle electronic content with at least a predefined level of security"; and (3) "determining, using the rights management engine, whether the one or more conditions specified by the data have been satisfied." PO Resp. 22–37; PO Sur-reply 3–11. We address Intertrust's arguments directed to each limitation in turn.

*a. "a condition that the piece of electronic content be rendered by a rendering application associated with a first digital certificate"*

In its Patent Owner Response, Intertrust contends that Peinado's license 16, which includes, among other things, security requirement 68 and trusted security value certifying authority 74, does not teach "the claimed condition that a rendering application be associated with a specific digital certificate" (i.e., a "first digital certificate"). PO Resp. 22–23 (citing Ex. 1007, 40:49–57, Fig. 8; Ex. 2033 ¶¶ 83–86). Intertrust argues that Peinado's license 16 "nowhere identifies a *specific* digital certificate that . . . rendering application [34] must be associated with." *Id.* at 24. Instead,

Intertrust argues that, before Peinado determines whether rendering application 34 is approved to render digital content 12, Peinado discloses extracting security value information 70, 70a, 70b, etc. and security value certifying authority 76 from certificate 72, and then comparing that information with security requirement 68 and trusted security value certifying authority 74 contained within license 16. *Id.* at 26–27 (citing Ex. 1007, 40:38–34, 40:42–48, Fig. 17 (steps 1709–15); Ex. 2034, 115:4–117:4 (Dr. Chatterjee deposition transcript); Ex. 2033 ¶¶ 90, 91).

Intertrust further contends that Peinado's extraction and comparison steps are distinguishable from independent claim 17 because this claim requires "a simpler method that confirms the presence of an appropriate digital certificate associated with the [rendering] application without the need to compare any security values." PO Resp. 27 (Ex. 1001, 5:54–57; Ex. 2033 ¶¶ 92, 93). Intertrust argues that the method of independent claim 17 is simpler and advantageous over Peinado's solution for the following two additional reasons: (1) independent claim 17 "does not require the user device to have (and maintain) algorithms to determine whether a given certifying authority and security value are sufficient"; and (2) Peinado's "determination that . . . rendering application [34] will handle electronic content with at least a predefined level of security occurs locally on the user device," whereas the determination required by independent claim 17 is made "by an entity that generates the certificate . . . that typically resides in a back-end location." *Id.* at 27–29 (citing Ex. 1001, 4:21–26, 7:64–8:2; Ex. 2033 ¶¶ 94, 95; Ex. 1002 ¶ 160). Intertrust then directs us to the embodiment illustrated in Figure 3B of the '106 patent as further support for its argument that the claimed "condition" requires a rendering application

associated with "a specific *digital certificate*." *Id.* at 29–31 (citing Ex. 1001, 6:33–61, Figs. 3B; Ex. 2033 ¶¶ 96, 97).

Lastly, Intertrust contends that Dolby's declarant, Dr. Chatterjee, erroneously testifies during cross-examination that Figure 6 of the '106 patent supports his opinion that independent claim 17 does not require that the rendering application be associated with a specific credential. PO Resp. 31 (citing Ex. 2034, 113:3–115:2). According to Intertrust, Figure 6 and its corresponding description demonstrate that the rights management engine checks whether the rendering application is associated with a specific certificate issued by entity ABC. *Id.* (citing Ex. 1001, 10:24–26, 11:20–23; Ex. 2033 ¶ 98). Intertrust also argues that the specification supports its reading of independent claim 17 as distinguishable from Peinado's solution because it conditions the use of content on certain characteristics of the rendering application, "without the necessity of explicitly including the details of these requirements in the controls that are directly associated with the content." *Id.* at 31–32 (emphasis omitted) (quoting Ex. 1001, 5:58–6:10).

In its Reply, Dolby contends that Peinado's rendering application 34 must meet certain security conditions, including that the rendering application be associated with certificate 72 issued from a trusted authority, before rendering digital content 12 and, therefore, teaches "a condition that the piece of electronic content be rendered by a rendering application associated with a first digital certificate," as recited in independent claim 17. Pet. Reply 3–4 (Ex. 1007, 17:60–67, 38:44–40:65, Fig. 17; Ex. 1002 ¶¶ 43–45, 87, 89, 90, 113–21, 141, 142). Dolby disagrees with Intertrust's arguments for several reasons, but primarily because, according to Dolby,

Intertrust mischaracterizes its asserted obviousness ground based on the teachings of Peinado and relies on an unduly narrow reading of independent claim 17. *Id.* at 4. First, Dolby argues that its asserted obviousness ground based on the teachings of Peinado does not just rely on Peinado's list of certifying authorities to teach the claimed "condition," but instead relies on comparing security value certifying authority 76 from certificate 72 with trusted security value certifying authority 74 contained within license 16. *Id.* at 4–5 (citing Dec. on Inst. 36; Pet. 43–47; Ex. 1002 ¶¶ 113–21).

Second, Dolby contends that Intertrust incorrectly suggests that Peinado's certificate 72 itself must set forth the additional conditions. Pet. Reply 5. According to Dolby, neither the plain language of independent claim 17 nor the specification of the '106 patent limit the claimed "first digital certificate" to one that must include additional conditions, but rather merely requires "receiving . . . *data* specifying one or more conditions . . . including a condition that the piece of electronic content be rendered by a rendering application associated with a first digital certificate." *Id.* (quoting Ex. 1001, 19:28–33) (omissions in original). Dolby argues that, because there is no dispute that Peinado's certificate 72 is a digital certificate associated with rendering application 34, "it is . . . irrelevant whether certificate 72 itself specifies additional conditions unrelated to an acceptable rendering application." *Id.*

Third, Dolby contends that Intertrust incorrectly suggests that the claimed "condition" requires a "specific digital certificate." Pet. Reply 6 (citing PO Resp. 23–24). According to Dolby, Intertrust's argument in this regard is predicated on an unduly narrow reading of the claimed "condition." *Id.* Dolby asserts that independent claim 17 does not recite a specific digital

certificate, much less that the data specifying the claimed "condition" identifies a specific digital certificate. *Id.* (citing Ex. 1001, 19:28–33). Dolby then reiterates that Peinado's extraction and comparison steps fall within the broad scope of the claimed "condition" because independent claim 17 does not place any restrictions as to how the claimed "condition" is expressed. *Id.* at 6–7.

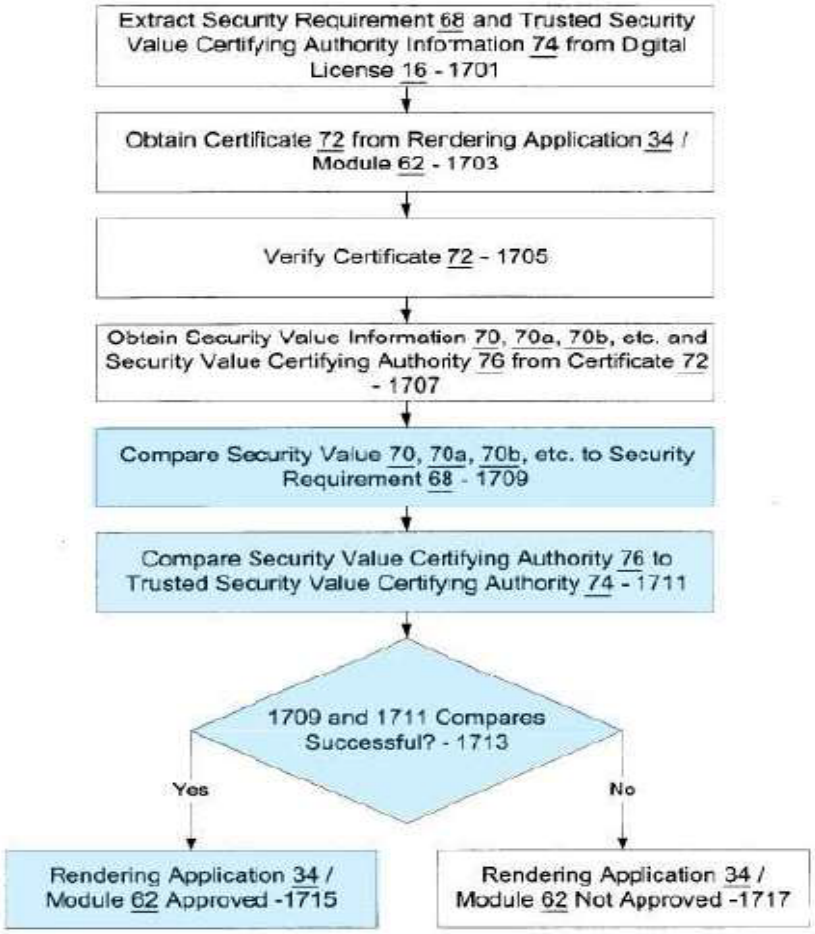
Lastly, Dolby disagrees with Intertrust's reliance on particular embodiments disclosed in the specification of the '106 patent to limit the scope of independent claim 17. Pet. Reply 7. Beginning with the embodiment illustrated in Figure 3B of the '106 patent, Dolby argues that Intertrust fails to recognize that this particular embodiment is consistent with Peinado's solution that requires comparing information contained within license 16 and certificate 72 because it explicitly requires "verif[ying] the integrity/authenticity of the credential and/or application" by "decrypting" and "comparing the output with a hash." *Id.* (citing PO Resp. 20 (quoting Ex. 1001, 6:38–44)) (alteration in original). Nevertheless, Dolby asserts that Intertrust fails to recognize that independent claim 17 is not limited to the particular embodiment illustrated in Figure 3B because the corresponding description of this embodiment contemplates other suitable methods for checking the credential of an application. *See id.* at 8 (citing Ex. 1001, 6:57–61). Turning to the embodiment illustrated in Figure 6 of the '106 patent, Dolby argues that Intertrust does not offer any argument or evidence to dispute Dr. Chatterjee's cross-examination testimony that Figure 6 discloses "one of the rules is that the rendering app must be certified by XYZ, which would be, for example, the trusted certifying authorities of Peinado." *Id.* at 8–9 (quoting Ex. 2034, 113:3–115:2).

In its Sur-reply, Intertrust reiterates its argument that Peinado's license 16 nowhere identifies a specific digital certificate that rendering application 34 must be associated with and, despite Dolby's arguments to the contrary, independent claim 17 does require a specific digital certificate—namely, a certificate generated in accordance with the express requirements of this claim. PO Sur-reply 8–9. Intertrust further contends that, although the embodiment illustrated in Figure 3B of the '106 patent contemplates the use of other suitable methods for checking the credential of an application, this does not mean that independent claim 17 covers all other methods, including the solution proposed by Peinado. *Id.* at 9. Relying on the testimony of its declarant, Dr. Jakobsson, Intertrust asserts that the embodiment illustrated in Figure 3B satisfies the "condition" required by independent claim 17. *Id.* (citing Ex. 2033 ¶¶ 96, 97). Intertrust also argues that Dolby incorrectly suggests that Peinado operates in the same way as independent claim 17. *Id.* As illustrated by steps 1705 through 1713 in Figure 17 of Peinado, Intertrust asserts that Peinado requires a multi-step process that is not required by independent claim 17 "to determine whether (1) the certification was generated by a trusted certifying authority, and (2) whether the application is sufficiently secure to render the content." *Id.* at 9–10 (citing Ex. 2033 ¶ 91). Lastly, Intertrust maintains its position that, during cross-examination, Dr. Chatterjee fails to appreciate that Figure 6 of the '106 patent and its corresponding description requires that the rendering application be associated with a specific digital certificate—certificate 606—before rendering content. *Id.* at 10 (citing Ex. 1001, 11:16–23; Ex. 2034, 113:9–15).

Based on the fully developed trial record, we agree with Dolby that Peinado's rendering application 34 must meet certain security conditions, including that it be associated with certificate 72 issued from a trusted authority, before rendering digital content 12. Pet. 45–47; Pet. Reply 3–4. Accordingly, we find that Peinado teaches "a condition that the piece of electronic content be rendered by a rendering application associated with a first digital certificate," as recited independent claim 17.

As an initial matter, the parties do not dispute that Figure 4 of Peinado illustrates that rendering application 34 is associated with certificate 72. Ex. 1007, 39:19–22, Fig. 4. We turn now to an annotated version of Figure 17 of Peinado, reproduced below, which illustrates the various steps performed during security approval of rendering application 34. *Id.* at 4:62–64; *see also id.* at 40:9–14 (describing security approval as DRM system 32 approving rendering application 34 for use in accordance with license 16).

**PEINADO, FIG. 17 (ANNOTATED)**




Pet. 47. This annotated version of Figure 17, reproduced above, illustrates how DRM system 32, which is contained within user's computing device 14, examines digital license 16 and extracts security requirement 68 and trusted security value certifying authority 74. Ex. 1007, 40:13–17 (Step 1701). Next, DRM system 32 obtains certificate 72 attached to rendering application 34 that includes security value information 70, 70*a*, 70*b*, etc. and indicia of security value certifying authority 76. *Id.* at 40:17–21, Fig. 17 (Steps 1703). DRM system 32 then verifies that certificate 72 is associated with rendering application 34 by comparing the following: (1) security

value information 70, 70*a*, 70*b*, etc. from certificate 72 with security requirement 68 obtained from license 16; and (2) security value certifying authority 76 from certificate 72 with trusted security value certifying authority 74 obtained from license 16. *Id.* at 40:21–48, Fig. 17 (Steps 1705–11). If both comparisons are successful, then DRM system 32 verifies that rendering application 34 meets the security conditions set forth in license 16, thereby approving the rendering application to render digital content 12. *Id.* at 40:49–57, Fig. 17 (Steps 1713 and 1715).

This process illustrated in Figure 17 by which DRM system 32 approves rendering application 34 for use in accordance with license 16 also finds support in other disclosures throughout Peinado. For instance, Peinado states that "the rights description in each license 16 specifies whether the user has rights to play . . . digital content 12 based on several factors," including, among other things, "what rendering application 34 is calling . . . DRM system 32." Ex. 1007, 17:61–67. As one example, Peinado states that "license 16 may appropriately specify that . . . rendering application 34 . . . must be from one or more particular sources/suppliers/developers." *Id.* at 38:44–49. Together, these two cited disclosures in Peinado further reinforce our finding that Peinado's rendering application 34 must meet certain security conditions, including that it be associated with certificate 72 issued from a trusted authority, before rendering digital content 12 and, therefore, teaches "a condition that the piece of electronic content be rendered by a rendering application associated with a first digital certificate," as recited in independent claim 17.

Dolby's declarant, Dr. Chatterjee, also provides testimony supporting our finding in this regard. In his Declaration accompanying the Petition,

Dr. Chatterjee testifies that "[t]rusted [c]ertifying [a]uthorities 74 in license 16 indicates which certifying authorities 76 can be trusted," and "[s]ecurity [r]equirement 68 in license 16 indicates what security values 70 in rendering application 34's certificate [72] are acceptable." Ex. 1002 ¶ 90 (emphasis omitted). According to Dr. Chatterjee, "[o]nly those rendering applications that satisfy these requirements in license 16 are approved for use by DRM system 32." *Id.* (emphasis omitted) (citing Ex. 1007, 38:55–40:65, Fig. 17). As one example of a condition imposed by Peinado's security approval process illustrated in Figure 17, Dr. Chatterjee testifies that "DRM system 32 examines certificate 72 of rendering application 34 by comparing the indicia of . . . certifying authority 76 in certificate 72 to the indicia specified in trusted security value certifying authority information 74." *Id.* ¶ 120 (citing Ex. 1007, 40:42–48, annotated version of Fig. 1). He testifies that "DRM system 32 'does not approve' . . . rendering application 34 if it does not meet the 'security criteria' of license 16." *Id.* ¶ 121 (citing Ex. 1007, 40:57–65, Fig. 17). Dr. Chatterjee then concludes his testimony on this particular issue by averring that the security "conditions [imposed by] [t]rusted [c]ertifying [a]uthorities 74 in license 16 require that content be rendered by a rendering application associated with a first digital certificate." *Id.* We credit the aforementioned testimony of Dr. Chatterjee because it is consistent with the disclosures in Peinado highlighted above, most notably the security conditions identified in the security approval process of rendering application 34 illustrated in Figure 17.

We do not agree with Intertrust's argument that the "first digital certificate" of independent claim 17 must be a "specific digital certificate." *See, e.g.*, PO Resp. 22 (arguing that Peinado's license 16 that includes a list

of trusted security value certifying authorities 74 does not teach the claimed "condition," much less a "specific digital certificate"), 24 (arguing that Peinado's license 16 "nowhere identifies a *specific* digital certificate"), 27 (arguing that Peinado's extracting and comparison steps do not disclose or even contemplate a "specific *digital certificate*"), 30 (arguing that the particular embodiment illustrated in Figure 3B of the '106 patent requires a "specific *digital certificate*"); PO Sur-reply 9 (arguing that independent claim 17 "does mandate use of a specific certificate"), 10 (arguing that independent claim 17 encompasses the particular embodiment illustrated in Figure 6 of the '106 patent that includes a rule that requires the application to be associated with a "specific digital certificate"—certificate 606). Independent claim 17 merely recites "a rendering application associated with a first digital certificate." Ex. 1001, 19:32–33. Apart for independent claim 17 further requiring "a first entity" that generates the "first digital certificate" based, at least in part, on a determination that the rendering application handles electronic content with at least a predefined security level, which we discuss in more detail below, this claim does not further limit the "first digital certificate" by requiring it to be a specific digital certificate, nor does this claim require that the claimed "condition" itself explicitly identify the "first digital certificate." *Id.* at 20:1–6.

We also do not agree with Intertrust's argument that independent claim 17 is distinguishable from the teachings of Peinado because it sets forth a "simpler method" than the security approval process of rendering application 34 illustrated in Figure 17 of Peinado. *See* PO Resp. 27–29. Intertrust's attempts to distinguish independent claim 17 from the relevant teachings of Peinado are based on the following three assertions:

(1) independent claim 17 confirms the presence of a digital certificate associated with a rendering application, without the need to compare security values; (2) independent claim 17 does not require the computing device to use or maintain algorithms; and (3) the determination in independent claim 17 that the rendering application handles digital content with at least a predefined level of security is made by an entity that generates the certificate who typically resides in a back-end location. *See id.* Intertrust's assertions, however, impermissibly seek to narrow the scope of the claimed "condition" recited in independent claim 17 either by reading in a negative limitation (i.e., without the need to compare security values and not requiring the computing device to use or maintain algorithms) or by reading in limitations that are not otherwise explicitly recited in this claim (i.e., requiring the entity that generates the certificate to reside in a back-end location).

Beginning with the negative limitations Intertrust attempts to improperly incorporate into its reading of the claimed "condition" of independent claim 17, we preliminarily determined—and the parties do not dispute—that the plain language of this limitation merely requires "a condition that the piece of electronic content be rendered by a rendering application associated with a first digital certificate," without placing specific restrictions as to how the claimed "condition" is expressed. Dec. on Inst. 36; *see also* Pet. Reply 6 (repeating our preliminary determination from the Decision on Institution and signifying agreement by emphasizing "without placing specific restrictions as to how the claimed 'condition' is expressed" (emphasis omitted)); PO Sur-reply 11 (stating that, "it is true, as the Board preliminarily found, that the claim does not 'plac[e] specific

restrictions as to how that claimed 'condition' is expressed" (alteration in original)). Given that independent claim 17 is broad in scope because it does not place specific restrictions as to how the claimed "condition" is expressed, we decline to require this limitation to include negative limitations, such as without the need to compare security values or not requiring the computing device to use or maintain algorithms. Stated differently, Intertrust engages in a *post hoc* attempt to import negative limitations into its reading of the claimed "condition" by impermissibly incorporating language, which, as far as we can discern, is not supported by the specification of the '106 patent. This attempt to incorporate extraneous features into the claimed "condition," of course, is improper.

Turning to the remaining limitations that Intertrust attempts to improperly incorporate into its reading of the claimed "condition" of independent claim 17, this claim merely recites that "the first digital certificate having been generated by a first entity." Ex. 1001, 20:3–4. Intertrust does not direct us to, nor can we find, any additional limitations recited in independent claim 17 that specifically require the first entity that generates the certificate to reside in a back-end location. Moreover, Figure 1 of the '106 patent illustrates a rights management system that includes credential authority 102 that defines certain requirements 103 that applications must meet to receive a credential. *Id.* at 3:46–48. The corresponding description of Figure 1, however, does not specify the location of credential authority 102, much less identify any benefits for managing security-related decisions in a back-end location. The only evidence Intertrust cites to support this argument is the testimony of its declarant, Dr. Jakobsson. PO Resp. 28–29 (citing Ex. 2033 ¶ 95).

Dr. Jakobsson, however, repeats verbatim the same conclusory assertions as the Patent Owner's Response, without providing additional evidentiary support. *Compare* Ex. 2033 ¶ 95, *with* PO Resp. 28–29.

Lastly, we do not agree with Intertrust's attempt to limit the claimed "condition" of independent claim 17 by relying on the particular embodiment illustrated in Figure 3B of the '106 patent. *See* PO Resp. 29–31; PO Sur-reply 9. The U.S. Court of Appeal for the Federal Circuit "has repeatedly 'cautioned against limiting the claimed invention to preferred embodiments or specific examples in the specification.'" *Williamson v. Citrix Online, LLC*, 792 F.3d 1339, 1346–47 (Fed. Cir. 2015) (quoting *Teleflex, Inc. v. Ficosa N. Am. Corp.*, 299 F.3d 1313, 1328 (Fed. Cir. 2002)). Significantly, "it is the claims, not the written description, which define the scope of the patent right." *Id.* at 1346 (quoting *Laitram Corp. v. NEC Corp.*, 163 F.3d 1342, 1347 (Fed. Cir. 1998) (alterations and emphasis removed); *see also* PO Sur-reply 9 ("The claim language, not the specification, controls."). In any event, even if we were to agree with Intertrust that the claimed "condition" of independent claim 17 encompasses the particular embodiment illustrated in Figure 3B, the specification of the '106 patent explicitly states that this embodiment is not so limiting. *See* PO Resp. 30 (emphasis omitted); PO Sur-reply 9. After describing the particular embodiment illustrated in Figure 3B, the '106 patent acknowledges that "[i]t will be appreciated that *other suitable methods* can be used for checking" the credential of an application. Ex. 1001, 6:57–61 (emphasis added).

*b. "the rendering application being associated with at least the first digital certificate, the first digital certificate having been generated by a first entity based at least in part on a determination that the rendering application will handle electronic content with at least a predefined level of security"*

In its Patent Owner Response, Intertrust contends that Peinado's digital certificate 72 that specifies the security level of rendering application 34 using a letter scale (e.g., A, B+, AAA, etc.) or numerical scale does not teach generating a certificate for the rendering application if it is determined that the rendering application handles content with at least a predefined level of security. PO Resp. 32–33. Instead, Intertrust argues that Peinado issues a digital certificate to all rendering applications, regardless of their security level and, therefore, must specify the security value in the digital certificate itself. *Id.* at 33 (citing Ex. 2033 ¶¶ 104). Stated differently, Intertrust argues that Peinado's system relies on the security value specified in the digital certificate associated with the rendering application to determine what rights to provide the rendering application. *Id.* (citing Ex. 2033 ¶¶ 105, 106). In contrast, Intertrust argues that independent claim 17 conditionally issues the first digital certificate associated with a rendering application "only if" the rendering application, among other things, renders electronic content with at least a predefined security level. *Id.* at 34.

Intertrust further contends that the relevant teachings of Peinado are distinguishable from independent claim 17 because Peinado generates security values for each rendering application that are not necessarily representative of how the rendering application handles electronic content. PO Resp. 34. According to Intertrust, Peinado relies on numerous factors when assigning rendering application security values, and many of these

factors have nothing to do with how the rendering application handles electronic content. *Id.* (citing Ex. 1007, 39:56–65; Ex. 2034, 128:10–129:1; Ex. 2033 ¶¶ 108, 109). Intertrust further argues that the inclusion of "based in part" language in independent claim 17 signifies that, in addition to checking the sufficiency of the rendering application's security attributes, a certificate authority may elect not to issue a certificate for a rendering application unless it has certain functional attributes to ensure, for example, that it will operate reliably. *Id.* at 35 (citing Ex. 2033 ¶¶ 110, 111). As a few examples, Intertrust directs us to application credential 812 illustrated in Figure 8 of the '106 patent, together with the disclosure in the specification that states "different levels of certification could be represented by different credentials assigned to the [rendering] application, or by different attributes specified in a single credential." *Id.* at 35–36 (quoting Ex. 1001, 15:59–61) (citing Ex. 1001, Fig. 8 (application credential 812 and attributes 814–818)).

In its Reply, Dolby contends that Peinado's certifying authority 76 determines the security level of the rendering application by considering several predetermined factors, such as whether it has a security value of at least a minimum threshold and, therefore, teaches generating certificate 72 based, at least in part, on whether the rendering application handles electronic content with at least a predefined security level. Pet. Reply 9–10 (citing Ex. 1007, 38:60–39:3, 39:19–25, 39:56–65; Pet. 48–51; Ex. 1002 ¶¶ 127–29). Dolby also argues that, at a minimum, it would have been obvious to a person of ordinary skill in the art to modify Peinado's certifying authority 76 to conditionally generate a certificate if the rendering application is determined to handle electronic content with at least a predefined security level. *Id.* at 10 (citing Pet. 50; Ex. 1002 ¶ 130).

Dolby further contends that Intertrust offers no basis to read the limitation at issue as requiring a conditional "only if" test before generating a digital certificate. Pet. Reply 10 (citing PO Resp. 32–37). Dolby argues that independent claim 17 does not include an "only if" requirement, nor does this claim include the word "conditionally." *Id.* Instead, Dolby argues that, as we recognized in our Institution Decision, the '106 patent contemplates generating a certificate for a rendering application in a manner that permits different levels of certification. *Id.* at 10–11 (citing Dec. on Inst. 37–38). According to Dolby, Intertrust does not dispute that the cited disclosure in the specification of the '106 patent is similar to the teachings of Peinado. *Id.* Moreover, Dolby argues that, even if we were to accept Intertrust's unduly narrow reading of the limitation at issue, Peinado discloses assigning certificate 72 to rendering application 34 using a letter scale (e.g., A, B+, AAA, etc.), each of which represents a predefined security level. *Id.* at 11–12 (citing Ex. 1002 ¶¶ 127–29). That is, Dolby asserts that rendering application 34 would receive an "A" rated certification only if it is determined that the rendering application meets or otherwise satisfies an "A" predefined security level. *Id.* at 12.

In its Sur-reply, Intertrust contends that recitation of the words "only if" or "conditionally" are not necessary to convey a conditional requirement if, as recited in independent claim 17, generating the digital certificate must be "based at least in part" on satisfying a condition. PO Sur-reply 3 (citing Ex. 2033 ¶¶ 110, 111). Intertrust, therefore, maintains that independent claim 17 requires generating the "first digital certificate" "only if" a determination is made that the rendering application handles electronic content with at least a predefined security level. *Id.* at 3–4. In contrast,

Intertrust argues that Peinado requires several additional processing steps, including the extraction and comparison steps, which make it far less efficient than the method of independent claim 17. *Id.* at 4–5.

Lastly, Intertrust contends that, even though the specification of the '106 patent contemplates generating a certificate for an application in a manner that permits different levels of certification, Dolby does not demonstrate that this disclosure falls within the scope of independent claim 17. PO Sur-reply 6. Intertrust asserts that independent claim 17 says nothing about different or multiple levels of certification, but instead explicitly recites a single "pre-defined level of security." *Id.*

Based on the fully developed trial record, we agree with Dolby that Peinado's certifying authority 76 determines the security level of rendering application 34 by considering several factors, including the particular developer of rendering application 34 and the history of trust that developer has established with regard to the rendering application (e.g., a minimum threshold of trust), prior to generating security values 70 using a letter and/or numerical scale that are specified in certificate 72. *See* Pet. 48–51; Pet. Reply 9–10. Accordingly, we find that Peinado teaches "the rendering application being associated with at least the first digital certificate, the first digital certificate having been generated by a first entity based at least in part on a determination that the rendering application will handle electronic content with at least a predefined level of security," as recited in independent claim 17.

As we explain previously, the parties do not dispute that Figure 4 of Peinado illustrates that rendering application 34 is associated with certificate 72. *See supra* Section II.B.4.a; Ex. 1007, 39:19–22, Fig. 4. Peinado

discloses that its approach of assigning rendering application 34 a certificate associated with a particular security level is "flexible and robust . . . [and] is not overly limiting." Ex. 1007, 38:55–59. In one embodiment, Peinado discloses that certifying authority 76 issues certificate 72 to rendering application 34 by determining "security value(s) 70 based on predetermined parameters." *Id.* at 39:22–25. Peinado then states that these predetermined parameters or factors include, among other things "the particular source/supplier/developer of" rendering application 34 and "what kind of history of trust has been established with regard to" rendering application 34. *Id.* at 39:56–65. Based on these and other factors, security values 70 may be specified in certificate 72 in a scaled manner, such as using letter scales (e.g., "A, A-, B+, B, etc.; AAA, AA, A, BBB, BB, etc.") or numerical scales (e.g., "a pre-assigned security value of at least 50, greater than 40, 20 or higher, or the like"). *Id.* at 38:66–39:14, 39:66–40:2.

Dolby's declarant, Dr. Chatterjee, also provides testimony supporting our finding in this regard. In his Declaration accompanying the Petition, Dr. Chatterjee testifies that "a person of ordinary skill in the art at the time of the alleged invention of the '106 patent would have known that letter grades such as A, B, C., etc. correspond to raw numerical test scores." Ex. 1002 ¶ 128. As just one example, he testifies that "[e]ach security value on the letter scale would correspond to a range of numerical values, *e.g.*, 'A' would correspond to 90-100, 'B' would correspond to 80-90, and so on." *Id.* Accordingly, he testifies that "a determination that rendering application 34 has a security value of 'A' means that it has a security value of at least 90." *Id.* We credit the aforementioned testimony of Dr. Chatterjee because it is consistent with the Peinado's approach of assigning rendering application 34

a certificate associated with a particular security level that is both "flexible and robust," which may include using security scales (e.g., a letter and corresponding numerical score). Moreover, Dr. Chatterjee's testimony on this particular issue, together with Peinado's disclosure of using letter and/or numerical scales to assign security values to certificate 72, also provides ample support for Dolby's assertion that Peinado's rendering application 34 would receive an "A"-rated certification only if it is determined that the rendering application meets or otherwise satisfies an "A" predefined security level. Pet. Reply 12.

We do not agree with Intertrust's argument that the words "only if" or "conditionally" should be treated as having the same scope of "based at least in part" recited in independent claim 17 such that this claim should be read as generating the "first digital certificate" "only if" a determination is made that the rendering application handles electronic content with at least a predefined security level. *See* PO Resp. 33–35; PO Sur-reply 3–4. In the Institution Decision, we preliminary determined that the language "based at least in part" is not so restrictive, but is broad enough to encompass assigning rendering applications different levels of certification, at least one of which being based on a "predefined" security level. Dec. on Inst. 37–38. Although we made this preliminary determination in the Institution Decision, during trial, Intertrust does not provide an adequate explanation and supporting evidence for us to treat the "based at least in part" language any differently for purposes of this Final Written Decision. That is, when considering the plain language of the independent claim 17 and the specification of the '106 patent, we decline to narrow the scope of the

"based at least in part" language by treating it as being equal to "only if," which is an absolute term not recited in independent claim 17.

We also do not agree with Intertrust's argument that the disclosure in the specification of the '106 patent of generating a certificate for a rendering application in a manner that permits different levels of certification has no bearing on the scope of "based at least in part" recited in independent claim 17. *See* PO Sur-reply 3, 6. The relevant disclosure in the specification states the following:

> The provider of the digital rights management system (or other secure client software), may issue a credential to applications certified by the provider as meeting certain security requirements. A lesser level of "certification" may be provided to applications that are merely capable of operating in connection with the secure processing software, but about which the provider makes no representations as to security. These different levels of certification could be represented by different credentials assigned to the application, or by different attributes specified in a single credential.

Ex. 1001, 15:52–61. Although this cited disclosure explicitly identifies "[t]he provider of the digital rights management system (or other secure client software)" as someone who issue certificates, we do not view this disclosure as only limited to a provider of the DRM system because it uses the language "may." Whether the provider of the DRM system (*id.* at 15:52–55) or credential authority 102 illustrated in Figure 1 (*id.* at 3:46–48) issues the certificate does not change the fact that the specification of the '106 patent clearly contemplates generating a certificate for an application in a manner that permits different levels of certification. This is important to highlight because it undermines Intertrust's main argument that independent claim 17 requires generating the "first digital certificate" "only if" a

determination is made that the rendering application handles electronic content with at least a predefined security level.

In any event, even if we were to accept Intertrust's argument that the scope of "based at least in part" recited in independent claim 17 is equivalent to "only if," Peinado still teaches the limitation at issue. As we explain previously, Peinado discloses that certifying authority 76 determines the security level of rendering application 34 by considering several factors prior to generating security values 70 using a letter and/or numerical scale that are specified in certificate 72. In the context of describing numerical security scales, Peinado discloses one example where "license 16 may require each rendering application 34 . . . [to] have a pre-assigned security value of at least 50, greater than 40, 20 or higher, or the like." Ex. 1007, 39:11–14. Applying the scenario where license 16 requires the pre-assigned security value to be at least 50, Peinado teaches the limitation at issue because it is capable of generating certificate 72 "only if" a determination is

made that rendering application 34 handles electronic content with at least a predefined security value of at least 50.[5]

*c. "determining, using the rights management engine, whether the one or more conditions specified by the data have been satisfied"*

In its Patent Owner Response and its Sur-reply, Intertrust relies on essentially the same arguments and evidence presented above with respect to claimed "condition" to rebut Dolby's explanation as to how the teachings of Peinado account for "determining, using the rights management engine, whether the one or more conditions specified by the data have been satisfied," as recited in independent claim 17. PO Resp. 22–32; PO Sur-reply 8–11. For the same reasons we identify above with respect to the claimed "condition," we do not agree with Intertrust's arguments. Instead, based on the fully developed trial record, we agree with Dolby—and we find—that Peinado teaches the "determining" step because it discloses that DRM system 32 verifies that rendering application 34 meets certain security conditions by, as one example, comparing the trusted security value

[5] In its Patent Owner Response, Intertrust contends that Peinado teaches away from specifying that rendering application 34 is from "one or more particular sources/suppliers/developers" because it also states that "such specifications are overly limiting in that they may unnecessarily exclude other (perhaps newer) sources/suppliers/developers." PO Resp. 37–38 (quoting Ex. 1007, 38:45–54). We need not address Intertrust's teaching away argument because, as we explain above, the teachings of Peinado, without the modifications proposed by Dolby, account for "the rendering application being associated with at least the first digital certificate, the first digital certificate having been generated by a first entity based at least in part on a determination that the rendering application will handle electronic content with at least a predefined level of security," as recited in independent claim 17.

certifying authority information 74 obtained from license 16 with the certifying authority 76 that issued certificate 72. Pet. 53–54 (citing Ex. 1007, 40:28–34, 40:49–57, Fig. 17 (steps 1709–15); Ex. 1002 ¶¶ 141, 142).

*d. Objective Indicia of Non-Obviousness*

In its Patent Owner Response, Intertrust contends that there is evidence of long-felt need, failure of others, industry praise, commercial success, and copying, which should be considered as objective indicia of non-obviousness. PO Resp. 62–66. For us to give substantial weight to objective indicia of obviousness or non-obviousness, a proponent must establish a nexus between the evidence and the merits of the claimed invention. *ClassCo, Inc., v. Apple, Inc.*, 838 F.3d 1214, 1220 (Fed. Cir. 2016). "[T]here is no nexus unless the evidence presented is 'reasonably commensurate with the scope of the claims.'" *Id.* (quoting *Rambus Inc. v. Rea*, 731 F.3d 1248, 1257 (Fed. Cir. 2013)).

A patentee is entitled to a presumption of nexus "when the patentee shows that the asserted objective evidence is tied to a specific product and that product 'embodies the claimed features, and is coextensive with them.'" *Fox Factory, Inc. v. SRAM, LLC*, 944 F.3d 1366, 1373 (Fed. Cir. 2019) (quoting *Polaris Indus., Inc. v. Arctic Cat, Inc.*, 882 F.3d 1056, 1072 (Fed. Cir. 2018)). But as Dolby correctly argues (Pet. Reply 23–25), a presumption of nexus is inappropriate here because Intertrust does not provide analysis demonstrating that its products are coextensive (or nearly coextensive) with the only challenged claim. *See Lectrosonics, Inc. v. Zaxcom, Inc.*, IPR2018-01129, Paper 33 at 33 (PTAB Jan. 24, 2020).

But even without the presumption, Intertrust "is still afforded an opportunity to prove nexus by showing that the evidence of secondary considerations is the 'direct result of the unique characteristics of the claimed invention.'" *Fox Factory*, 944 F.3d at 1373–74 (quoting *In re Huang*, 100 F.3d 135, 140 (Fed. Cir. 1996)). Also, the nexus must be "to some aspect of the claim *not already in the prior art*." *In re Kao*, 639 F.3d 1057, 1069 (Fed. Cir. 2011) (emphasis added). "Ultimately, the fact finder must weigh the [objective indicia] evidence presented in the context of whether the claimed invention as a whole would have been obvious to a skilled artisan." *Lectrosonics*, IPR2018-01129, Paper 33 at 33 (citing *WBIP, LLC v. Kohler Co.*, 829 F.3d 1317, 1331–32 (Fed. Cir. 2016)).

As we discuss below, we find that Intertrust has not shown a nexus between the claimed invention of the '106 patent and the purported evidence of long-felt need, failure of others, industry praise, commercial success, or copying. Although Intertrust comes closest to showing a nexus for industry praise, even if we were to find that there is a nexus, the evidence of industry praise does not outweigh the other evidence considered as part of the *Graham* factors.

Moreover, in addition to this proceeding, Intertrust presents nearly the same arguments and evidence with respect to objective indicia of non-obviousness in at least four other proceedings involving different patents. *See Dolby Laboratories, Inc. v. Intertrust Techs. Corp.*, IPR2020-00661, Paper 17 at 63–68 (PTAB Jan. 21, 2021) (Patent Owner Response); *Dolby Laboratories, Inc. v. Intertrust Techs. Corp.*, IPR2020-00662, Paper 17 at 60–65 (PTAB Jan. 21, 2021) (Patent Owner Response); *Dolby Laboratories, Inc. v. Intertrust Techs. Corp.*, IPR2020-00664, Paper 15 at 63–66 (PTAB

Mar. 2, 2021) (Patent Owner Response); *Dolby Laboratories, Inc. v. Intertrust Techs. Corp.*, IPR2020-01123, Paper 18 at 42–45 (PTAB Apr. 20, 2021) (Patent Owner Response). Intertrust, however, does not explain adequately how the same evidence of objective indicia of non-obviousness can be attributable to each particular claimed invention. *See Fox Factory*, 944 F.3d at 1378 ("The same evidence of secondary considerations cannot be presumed to be attributable to two different combinations of features. In such situations, the patentee retains the burden of proving the degree to which evidence of secondary considerations tied to a product is attributable to a particular claimed invention." (citation omitted)).

*i. Long-Felt Need and Failure of Others*

In order to show a long-felt but unmet need for the claimed invention, the objective evidence must show that the need was a persistent one that was recognized by those of ordinary skill in the art at the time of the invention. *In re Gershon*, 372 F.2d 535, 538 (CCPA 1967). As evidence of long-felt need and failure of others, Intertrust submits three articles from the *Wall Street Journal* which, according to Intertrust, suggest a need for a way to distribute digital content in a secure manner that would "(1) ensure the digital content would only be used in an authorized manner, (2) ensure that the digital content creator would be compensated for use of the digital content, and (3) allow for such distribution to client devices that were not under the control of the distributor." PO Resp. 63 (citing Ex. 2038, 1; Ex. 2039, 1; Ex. 2040, 1). Intertrust also submits another article from the *Wall Street Journal*, and an article from the *New York Times*, describing work by Xerox PARC, IBM, Microsoft, and other companies in the area of digital rights management. *Id.* at 63–64 (citing Ex. 2041, 3; Ex. 2042, 1).

Intertrust contends that "most, if not all, systems developed by others were either not commercially successful, were not adopted by digital content industries, copied the claimed invention or have been licensed under the claimed invention." PO Resp. 64. But Intertrust does not cite any evidence supporting this argument. We assign this evidence little weight, because Intertrust has not identified anything in the cited articles that ascribes any long-felt need to the merits of the claimed invention of the '106 patent, and has not pointed to any evidence that others had failed to achieve a solution to any technical problem for which the invention of '106 patent is also a solution.

*ii. Industry Praise*

As evidence of industry praise, Intertrust submits an article published in *Fortune*. PO Resp. 64–65 (citing Ex. 2044). Intertrust argues that the article praises its technology for "wrap[ping] the file in a secure digital container and tag[ging] it with rules describing how it could be used," and where, "[t]o play or read the . . . file, recipients would need special software or hardware that could be trusted by the content originator to enforce the rules." *Id.* at 65–66 (alterations and omission in original) (emphasis omitted) (quoting Ex. 2044, 2). According to Intertrust, these features are consistent with independent claim 17, "which requires that a 'rights management engine' determine that the one or more specified conditions have been satisfied such that the electronic content can be decrypted and rendered." *Id.* at 66 (emphasis omitted) (quoting Ex. 1001, claim 17).

In its Reply, Dolby contends that the *Fortune* article merely provides "a profile on [Intertrust] and an analysis of the legal battle between [Intertrust] and Microsoft." Pet. Reply 24. Dolby argues that the discussion

of wrapping content in a "secure digital container" tagged with rules does not address the claimed invention of the '106 patent, much less any aspect of independent claim 17. *Id.*

We determine that the *Fortune* article fails to provide a nexus to the claimed invention because Intertrust does not explain adequately how the article's discussion of wrapping a file in a secure digital container and tagging it with rules is coextensive with "rights management engine" recited in independent claim 17. Moreover, in this proceeding, Intertrust does not contest Dolby's arguments and evidence that Peinado's DRM system 32 teaches the "rights management engine" of independent claim 17. *See* PO Resp. 22–37. "Where the offered secondary consideration actually results from something other than what is both claimed and *novel* in the claim, there is no nexus to the merits of the claimed invention." *Kao*, 639 F.3d at 1068. Thus, we find that Intertrust has not shown that there is a nexus between the evidence of industry praise and the merits of the claimed invention. Absent a nexus, we assign little weight to the evidence of industry praise.

*iii. Commercial Success and Copying*

As evidence of commercial success and copying, Intertrust argues that over two dozen companies have licensed the claimed invention, and that "Intertrust has received more than $1 billion in licensing revenue in return for granting licensees the right to practice the claimed invention and Intertrust's remaining patent portfolio." PO Resp. 66.

But, once again, Intertrust does not cite any evidence to support its contention, such as the aforementioned licenses themselves, or any testimony by someone who was familiar with the circumstances of the licenses to Intertrust's portfolio. Absent such evidence, we cannot assess

whether the licenses have any nexus to the limitations of the only challenged claim. Thus, we assign little weight to Intertrust's unsupported arguments on commercial success and copying.

*e. Summary*

After weighing all of the evidence of obviousness and non-obviousness, on balance, Dolby has demonstrated by a preponderance of the evidence that the subject matter of independent claim 17 would have been obvious over the teachings of Peinado.

*C. Obviousness Over the Combined Teachings of Peinado and Shear*

Dolby contends that independent claim 17 of the '106 patent is unpatentable under § 103(a) as obvious over the combined teachings of Peinado and Shear. Pet. 56–61. Dolby explains how the teachings of Peinado and Shear account for the subject matter of this challenged claim, and provides reasoning as to why a person of ordinary skill in the art would have been prompted to combine the teachings of these two references. Pet. 56–61; Pet. Reply 13–15. Dolby also relies on the Declaration of Dr. Chatterjee accompanying the Petition to support its positions. Ex. 1002.

During trial, Intertrust contends that the combined teachings of Peinado and Shear do not account for all the limitations of independent claim 17 and Dolby fails to provide a sufficient rationale to combine the teachings of Peinado with those of Shear. PO Resp. 37–42; PO Sur-reply 11–12. Intertrust relies on the Declaration of Dr. Jakobsson accompanying the Patent Owner Response to support its positions. Ex. 2033.

We begin our analysis with a brief overview of Shear, and then we address the parties' contentions with respect to independent claim 17.

*1. Overview of Shear*

Shear generally relates to "bringing the efficiencies of modern computing and networking to the administration and support of electronic interactions" and, in particular, "to a 'Distributed Commerce Utility'—a foundation for the administration and support of electronic commerce and other electronic interaction and relationship environments." Ex. 1006, 1:8–16. More specifically, Shear discloses "[c]ertifying authority 500 [that] issues digital certificates 504 that certify particular facts." *Id.* at 71:11–12; Fig. 13. As one example, Shear discloses that certifying authority 500 is capable of issuing certificate 504 "to a computer attesting to the fact that the computer has a certain level of security." *Id.* at 72:19–22.

*2. Claim 17*

Dolby relies on the same arguments and evidence discussed above in its obviousness ground based on the teachings of Peinado alone to account for all the limitations of independent claim 17. Pet. 56. Nevertheless, Dolby argues that, to the extent Peinado does not teach "the rendering application being associated with at least the first digital certificate, the first digital certificate having been generated by a first entity based at least in part on a determination that the rendering application will handle electronic content with at least a predefined level of security," Shear teaches this limitation because it discloses generating a certificate based on a determination that a computer handles content with at least a certain security level. *Id.* at 56–58 (citing Ex. 1006, 71:6–8, 71:11–14, 72:19–22, 198:12–20, 199:25–200:6, Fig. 13; Ex. 1002 ¶¶ 147–58).

Turning to rationale to combine, Dolby contends that a person of ordinary skill in the art would have been motivated to apply Shear's

disclosure of generating a certificate based on a determination that a computer has a certain security level to Peinado's certificate generation process for rendering application 34 because it would have resulted in certain benefits. Pet. 58–60. For example, Dolby argues that combining the teachings of Peinado with those of Shear would exclude rendering applications whose security level is below a predefined security level, account for the preferences of particular content providers, ensure more efficient utilization of computational resources, and prevent exposure to security risks. *Id.* (citing Ex. 1002 ¶¶ 158–62). In addition, Dolby contends that combining the teachings of Peinado with those of Shear "would be nothing more than reorganizing familiar elements (certificates) according to known methods (known generation of certificates based on a threshold [security level]) to yield predictable results (generate a certificate based at least in part on a determination that the rendering application will handle content with at least a predefined [security level])." *Id.* at 60 (citing Ex. 1002 ¶ 163; *KSR*, 550 U.S. at 415–21). Lastly, Dolby argues that a person of ordinary skill in the art would have had a reasonable expectation of success in modifying the teachings of Peinado with those of Shear because Peinado's certifying authority 76 already assesses the security value of rendering application 34 and modifying that process to screen or reject rendering applications that do not meet a predefined security level would require only routine skill in the art. *Id.* at 60–61 (citing Ex. 1002 ¶ 165).

During trial, Intertrust presents arguments that raise the following two issues: (1) whether the combined teachings of Shear and Peinado account for "the rendering application being associated with at least the first digital certificate, the first digital certificate having been generated by a first entity

based at least in part on a determination that the rendering application will handle electronic content with at least a predefined level of security," as recited in independent claim 17; and (2) whether Dolby presents a sufficient rationale to combine the teachings of Peinado with those of Shear. PO Resp. 38–42; PO Sur-reply 11–12. We address Intertrust's arguments in turn.

*a. the rendering application being associated with at least the first digital certificate, the first digital certificate having been generated by a first entity based at least in part on a determination that the rendering application will handle electronic content with at least a predefined level of security"*

In its Patent Owner Response, Intertrust contends that Dolby and its declarant, Dr. Chatterjee, both overlook that Shear's disclosure of attesting to the security level of a computer is not the same as attesting to the security level with which a rendering application handles electronic content. PO Resp. 38 (citing Ex. 2034, 180:13–21, 181:10–13). According to Intertrust, Dolby does not cite to any disclosure in Shear "that relates to issuing a digital certificate associated with a rendering application, let alone a certificate attesting that the rendering application will handle electronic content with at least a predefined level of security." *Id.* at 38–39.

In its Reply, Dolby contends that Intertrust's argument mischaracterized its obviousness ground based on the combined teachings of Peinado and Shear. Pet. Reply 14. Dolby argues that Intertrust merely criticizes Shear's disclosure for lacking a "rendering application," but fails to appreciate that Dolby only relies on Shear's teaching of issuing certificates when a predefined security level is met. *Id.* Dolby also notes that, in the Institution Decision, we recognized that Shear's teachings are not limited to issuing certificates for just computers, but instead "[t]he only

restriction imposed on Shear's certifying authority 500 is that it issues 'digital certificates 504 that certify particular facts.'" *Id.* (citing Dec. on Inst. 42–43 (quoting Ex. 1006, 71:11–12)) (alteration in original). Relying on the testimony of Dr. Chatterjee, Dolby maintains that a person of ordinary skill in the art would have applied Shear's disclosure of only issuing certificate 504 if a predetermined security threshold is met to Peinado's digital certification procedure. *Id.* at 15 (citing Pet. 58–59; Ex. 1002 ¶¶ 158–62).

As an initial matter, we do not agree with Intertrust's argument because, as we explain previously, the teachings of Peinado alone account for "the rendering application being associated with at least the first digital certificate, the first digital certificate having been generated by a first entity based at least in part on a determination that the rendering application will handle electronic content with at least a predefined level of security," as recited in independent claim 17. *See supra* Section II.B.4.b. Consequently, there are no deficiencies in Peinado for Shear to remedy. In any event, assuming for purposes of argument that we agree with Intertrust that Peinado does not teach generating a certificate based, at least in part, on a determination that the rendering application handles electronic content with at least a predefined security level, we agree with Dolby that combined teachings of Peinado and Shear properly account for this limitation. That is, when applying Shear's disclosure of certifying authority 500 issuing certificate 504 attesting to a certain security level, we find that Peinado's certifying authority 76 would be capable of generating a certificate for Peinado's rendering application 34 attesting that the rendering application

handles digital content with at least a predefined security level. *See* Pet. 56–58.

Based on the fully developed trial record, we do not agree with Intertrust's argument that Shear's certifying authority 500 issuing certificate 504 attesting to a certain security level only applies to issuing certificates to computers and is not related to issuing digital certificates to rendering applications. *See* PO Resp. 38–39. Shear discloses that certifying authority 500 is capable of issuing certificates to organizations, machines, and people. Ex. 1006, 72:13–18. By use of the language "for example," Shear clearly identifies a computer as just one example of a component capable of receiving certification from certifying authority 500. *Id.* at 72:19–22. Indeed, based on our view of Shear's relevant disclosure, the only restriction imposed on Shear's certifying authority 500 is that it issues "digital certificates 504 that certify particular facts." *Id.* at 71:11–12. These cited disclosures in Shear, together with the supporting testimony of Dr. Chatterjee, amount to sufficient evidence that a person of ordinary skill in the art would have appreciated that Shear's disclosure of certifying authority 500 issuing certificate 504 attesting to a certain security level has common applications in computer technology, including with respect to software components such as Peinado's rendering application 34. *See* Ex. 1002 ¶¶ 158–63.

*b. Rationale to Combine*

In its Patent Owner Response, Intertrust contends that Dolby engages in impermissible hindsight reconstruction because, according to Intertrust, Dolby does not explain adequately why a person of ordinary skill in the art would have been motivated to modify Peinado's digital certification

procedure in a manner that would eliminate the very advantages espoused by Peinado. PO Resp. 40. Intertrust argues that Peinado provides a "flexible and robust [security type] that is not overly limiting" and this is achieved by assigning every rendering application a numerical security value in a scaled manner. *Id.* (quoting Ex. 1007, 38:55–39:3) (alteration in original). According to Intertrust, Dolby's proposed combination of Peinado and Shear would effectively eliminate Peinado's numerically scaled security values, and require a person of ordinary skill in the art to replace Peinado's entire digital certification procedure with one taught by the '106 patent. PO Resp. 40 (citing Ex. 2033 ¶ 118); *see also* PO Sur-reply 11–12 (citing Ex. 2033 ¶¶ 118, 119) (arguing the same). In addition, Intertrust contends that Dolby fails to provide a credible explanation as to why a person of ordinary skill in the art would have looked to the teachings of Shear because, according to Intertrust, Shear generally relates to certifying authority 500 attesting to certain facts, such as whether a computer has a certain security level, but Shear has nothing to do with rendering applications or imposing limitations on the rendering of digital content. PO Resp. 41 (citing Ex. 2033 ¶ 119).

In its Reply, Dolby contends that it does not rely on impermissible hindsight reconstruction, but explains at length in its Petition how combining the teachings of Shear with those of Peinado "would be nothing more than combining familiar elements (i.e., Peinado's certifying authority 76 issuing certificate 72 to rendering application 34) according to known methods, as taught by Shear (i.e., Shear's certifying authority 500 issuing certificate 504 that attests to the certified component having a certain level of security) to yield predictable results." Pet. Reply 15 (citing Pet. 58–61; Ex. 1002 ¶¶ 158–66).

The Supreme Court has held that an obviousness evaluation "cannot be confined by a formalistic conception of the words teaching, suggestion, and motivation, or by overemphasis on the importance of published articles and the explicit content of issued patents." *KSR*, 550 U.S. at 419. Instead, the relevant inquiry here is whether, based on the evidence available at trial, there is "some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006), *cited with approval in KSR*, 550 U.S. at 418. When describing examples of what may constitute a sufficient rationale to combine, the Court held that "[t]he combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results." *KSR*, 550 U.S. at 416 (followed by a discussion of cases that illustrate the application of this doctrine).

Based on the fully developed trial record, we agree with Dolby's asserted motivation for combining the teachings of Peinado with those of Shear because it rationally leads to the legal conclusion of obviousness. More specifically, we agree with Dolby that its proposed combination would have been nothing more than combining familiar elements (i.e., Peinado's certifying authority 76 issuing certificate 72 to rendering application 34) according to a known method (i.e., Shear's certifying authority 500 issuing certificate 504 attesting to a certain security level) to yield predictable results (i.e., Peinado's certifying authority 76 issuing certificate 72 to rendering application 34 if it meets a predefined security level). *See* Pet. 60; Pet. Reply 15. Intertrust does not address squarely this rationale to combine in either its Patent Owner Response or its Sur-reply, nor does Intertrust proffer any evidence to undermine this particular justification for obviousness. *See*

PO Resp. 40–43; PO Sur-reply 11–12. Moreover, contrary to Intertrust's assertion that Dolby engages in impermissible hindsight reconstruction, Dolby's position has a sufficient basis in the teachings of Peinado and Shear and it is supported by the testimony of Dr. Chatterjee. *See* Ex. 1006, 71:6–8, 71:11–14, 72:19–22, Fig. 13; Ex. 1007, 38:55–40:8; Ex. 1002 ¶¶ 158–63.

We do not agree with Intertrust's argument that Dolby's proposed combination of Peinado and Shear would effectively eliminate Peinado's numerically scaled security values, and would require a person of ordinary skill in the art to replace Peinado's entire digital certification procedure with one taught by the '106 patent. *See* PO Resp. 40; PO Sur-reply 11–12. Intertrust's argument is predicated on the notion that Dolby's proposed modification to Peinado requires eliminating Peinado's entire digital certification procedure. This mischaracterizes Dolby's proposed combination, which merely requires modifying Peinado's certifying authority 76 so that it issues certificate 72 to rendering application 34 if it meets a certain security level in the manner taught by Shear. Despite Intertrust's assertion to the contrary, Peinado's disclosure of providing a digital certification procedure that is "flexible and robust" and "not overly limiting" does not undermine its proposed combination with the teachings of Shear, but in our view supports modifying Peinado in the manner proposed by Dolby because Peinado promotes flexibility and avoids narrowing features. Ex. 1007, 38:55–59.

*c. Objective Indicia of Non-Obviousness*

Intertrust relies on the same evidence of long-felt need, failure of others, industry praise, commercial success, and copying as objective indicia of non-obviousness to rebut Dolby's asserted obviousness ground based on

the combined teachings of Peinado and Shear. PO Resp. 62–66. For the same reasons we identify above in the context of analyzing the asserted obviousness ground based on the teachings of Peinado alone, we assign little weight to this evidence. *See supra* Section II.B.4.d.i–iii.

*d. Summary*

After weighing all of the evidence of obviousness and non-obviousness, on balance, Dolby has demonstrated by a preponderance of the evidence that the subject matter of independent claim 17 would have been obvious over the combined teachings of Peinado and Shear.

*D. Remaining Obviousness Grounds*

Our conclusions that Dolby has demonstrated by a preponderance of the evidence that the subject matter of independent claim 17 would have been obvious over the teachings of Peinado alone and in combination with the teachings of Shear, renders it unnecessary for us to reach the remaining obviousness grounds based, in part, on the teachings of Hurtado. *Cf. In re Gleave*, 560 F.3d 1331, 1338 (Fed. Cir. 2009) (not reaching other grounds of unpatentability after affirming a ground based on anticipation); *see also Beloit Corp. v. Valmet Oy*, 742 F.2d 1421, 1423 (Fed. Cir. 1984) (explaining that an administrative agency is at liberty to reach a decision based on a dispositive issue because doing so "can not only save the parties, the [agency], and [the reviewing] court unnecessary cost and effort," but "can greatly ease the burden on [an agency] commonly faced with a . . . proceeding involving numerous complex issues and required by statute to reach its conclusion within rigid time limits").

## III. CONCLUSIONS[6]

Based on the fully developed trial record, Dolby has demonstrated by a preponderance of the evidence that independent claim 17 is unpatentable under § 103(a) as obvious. A summary of our conclusions is set forth in the table below.

| Claims | 35 U.S.C. § | Reference(s)/ Basis | Claims Shown Unpatentable | Claims Not Shown Unpatentable |
|---|---|---|---|---|
| 17 | 103(a) | Peinado | 17 | |
| 17 | 103(a) | Peinado, Shear | 17 | |
| 17 | 103(a) | Hurtado, Peinado[7] | | |
| 17 | 103(a) | Hurtado, Peinado, Shear[8] | | |
| **Overall Outcome** | | | 17 | |

[6] Should Intertrust wish to pursue amendment of the challenged claims in a reissue or reexamination proceeding subsequent to the issuance of this Decision, we draw Intertrust's attention to the April 2019 Notice Regarding Options for Amendments by Patent Owner Through Reissue or Reexamination During a Pending AIA Trial Proceeding. *See* 84 Fed. Reg. 16,654 (Apr. 22, 2019). If Intertrust chooses to file a reissue application or a request for reexamination of the challenged patent, we remind Intertrust of its continuing obligation to notify the Board of any such related matters in updated mandatory notices. *See* 37 C.F.R. § 42.8(a)(3), (b)(2).

[7] We already determined independent claim 17 to be unpatentable based on two other asserted grounds. As a result, we determine it is unnecessary to reach this asserted ground. *See Gleave*, 560 F.3d. at 1338.

[8] *See supra* n.7.

## IV. ORDER

In consideration of the foregoing, it is

ORDERED that independent claim 17 of the '106 patent is held to be unpatentable; and

FURTHER ORDERED that, because this is a Final Written Decision, parties to this proceeding seeking judicial review of our decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.

For PETITIONER:

Scott A. McKeown
Mark D. Rowland
Shrut Kirti
ROPES & GRAY LLP
scott.mckeown@ropesgray.com
mark.rowland@ropesgray.com
shrut.kirti@ropesgray.com

Leslie Spencer
DESMARAIS LLP
lspencer@desmaraisllp.com

For PATENT OWNER:

Christopher Mathews
Razmig Messerian
James M. Glass
Tigran Guledjian
Scott Florance
Iman Lordgooei (admitted *pro hac vice*)
QUINN EMANUEL URQUHART & SULLIVAN LLP
chrismathews@quinnemanuel.com
razmesserian@quinnemanuel.com
jimglass@quinneemanual.com
tigranguledjian@quinnemanuel.com
scottflorance@quinnemanuel.com
imanlordgooei@quinnemanuel.com